Testimony Of

DAVID AUCSMITH
CHIEF SECURITY ARCHITECT
INTEL CORPORATION

On Behalf Of The

BUSINESS SOFTWARE ALLIANCE

THE NEED FOR FUNDAMENTAL REFORM OF AMERICA'S ENCRYPTION POLICY

Before The

COMMERCE, SCIENCE AND TRANSPORTATION COMMITTEE
OF THE
U.S. SENATE

Washington, D.C.

June 10, 1999

SUMMARY OF STATEMENT OF DAVID AUCSMITH
CHIEF SECURITY ARCHITECT FOR INTEL CORPORATION

Thank you Mr. Chairman for the opportunity to talk to you this morning about the need for fundamental reform of America's encryption policy. I am pleased to appear today on behalf of the Business Software Alliance which, together with ACP, has been in the forefront of efforts to persuade the U.S. government to adopt a new U.S. encryption policy. **We urge the Committee to pass the PROTECT Act with further amendments that would make the bill more fully comport with technological and market realities.**

This morning I would like to briefly make five points that we believe should underpin U.S. encryption policy.

<u>First</u>, encryption is essential to <u>all</u> business in an Internet economy. While private sector interest in encryption export reform is generally characterized in terms of the competitiveness of American encryption products in a worldwide market, it is becoming a much larger issue for all American business. The global economy, tied together with the Internet, is turning businesses into virtual enterprises, localized products into global products, and geographically limited networks into worldwide networks. In this environment, American businesses must be able to sell and support their products worldwide, must be able to securely coordinate with their business partners worldwide, and must be able to conduct safe electronic commerce worldwide.

Quite simply, cryptography has emerged as the only possible solution to many of the requirements of commercial security. It is the essential building block for building trust onto the open Internet. Without it, the hundreds of billions of dollars of e-commerce currently projected to occur by the year 2002 will not happen.

<u>Second</u>, encryption is vital to securing America's critical infrastructures. Much of the national economy is at risk from the decisions that are made today on the issues of infrastructure protection. Increasingly, these critical systems are driven by, and linked together with, computers making them vulnerable to disruption. The single best way, and sometimes the only way to affect effectively these critical networks and systems, is encryption. That's why the National Research Council found that encryption promotes the national security of the United States. However, the security of any network is only as good as its weakest link. America's infrastructures cannot be protected if they are networked with foreign infrastructures using weak encryption.

<u>Third</u>, the availability of encryption cannot be reasonably controlled. Cryptography is a branch of mathematics. Cryptographic technology can be reduced to mathematical formulas and protocols. Information about cryptography is available from many sources in many forms. It is the subject of numerous academic conferences. It is taught in universities worldwide. Moreover, while developing good algorithms is tough, implementing them is relatively easy.

<u>Fourth</u>, government promoted or required plaintext access will not work. While required plaintext access offers, at first glance, a solution to the government's problem: (1) it is not technically possible in most circumstances; (2) it does not let law enforcement verify compliance with access requirements; and (3) it does not give national security interests access to stored keys. There is simply no way that law enforcement can determine, in advance, that particular text had not been encrypted with more than one program or product. At the same time, targets of national security interests are unlikely to design or use a plaintext infrastructure which would allow the U.S. government to have secret access to plaintext.

Moreover, there is practically no commercial reason for storing communications keys – if the communication is disrupted or compromised a new session will be established. At the same time, the need for key recovery of stored data also is overstated – the frequent example is an employee hit by a bus. With the exception of personal notes, information is not solely possessed by an individual. In addition, most mission-critical data is held by the corporate data management system that has its own control and protection mechanism. Finally, most personal data has a time value and rapidly becomes obsolete.

If one factors in the additional costs and systemic vulnerabilities that result from building in access features, we conclude that there is no business or consumer need for key recovery or special plaintext access. To be blunt: Intel does not plan to implement a key recovery scheme for its own use.

Fifth, the government needs to find technological alternatives to meet its requirements for access to information. Intel agrees that access to data communications and stored data by law enforcement intelligence communities is both legitimate and extremely important. Clearly, Congress should adequately fund the technical efforts of these agencies so they can meet the challenges of the next century. Industry supports additional funding. Industry can also provide other assistance.

For example, ACP proposed last year the creation of a "NET center" to help law enforcement officials understand how to deal with encryption and other technological advances. ACP also has advocated that the U.S. government should work cooperatively with our nation's hardware and software manufacturers to develop the technical tools and know-how that they need. Technical innovation is predominantly centered in the private sector – only a government/industry cooperative effort can address effectively the challenge of continued technological change.

In conclusion, **let me say that we strongly believe the Protect Act should be passed but with further improvements**.

The Protect Act does begin to realize the realities of mass market products, eliminates reporting requirements for such products, and grants export control relief to products at all horizontal layers in the information technology sector. But the Act still does not grant widespread exportability for mass market and publicly available encryption products. There is a complicated, bureaucratic process which must be pursued. Not until 2002 will American industry be able to widely export products using the 128-bit Advanced Encryption Standard or its equivalent.

We believe it is in our national interest to permit such exportability now and urge the Committee to amend the bill accordingly.

Once again, many thanks for this opportunity to testify.

INTRODUCTION.

My name is David Aucsmith, and as Chief Security Architect for the Intel Corporation I am responsible for research, development and deployment of data and communications security technologies and products, both hardware and software. Currently, my work is focusing on developing industry standard architectures for the application and interoperability of data security technologies for communications, electronic commerce, and content protection. I previously worked on security matters for two computer companies and as a Lieutenant Commander in Naval Intelligence.

Intel is the world's largest semiconductor manufacturer and a major supplier of information technology building blocks to the global computer and communications industries. We provide our customers with chips, printed circuit board assemblies and software that are the "ingredients" of PC's, servers and workstations. Our flagship business involves the mass production and sale of the Pentium® family of processors and other microprocessors, which are frequently described as the "brains" of a computer because they control the central processing of data in computers. In 1998, our sales exceeded $26 billion, and we employed more than 40,000 people in the United States.

Like most information technology companies, Intel's business model is global in scope. The bulk of our production takes place in the United States. Our products are sold worldwide to original equipment manufacturers of computer systems and peripherals, PC users who make purchases through various distribution channels including the Internet, and other manufacturers who produce a wide range of industrial and telecommunications equipment. Information security plays a prominent role in the conduct of our business.

Intel is headquartered in Santa Clara, California, and we have significant manufacturing facilities in a number of states, including Arizona, New Mexico, Oregon, California and Massachusetts.

Intel Corporation is a member of the Business Software Alliance ("BSA") and Americans for Computer Privacy ("ACP"). Both associations have been in the forefront of efforts to persuade the government to adopt a new encryption policy.

Since 1988, BSA has been the voice of the world's leading software developers before governments and with consumers in the international marketplace. BSA promotes the continued growth of the software industry through its international public policy, education and enforcement program in 65 countries throughout North America, Europe, Asia and Latin America. Its members represent the fastest growing industry in the world. BSA worldwide members include Adobe, Attachmate, Autodesk, Bentley Systems, Corel Corporation, Lotus Development, Macromedia, Microsoft, Network Associates, Novell, Symantec and Visio. Additional members of BSA's Policy Council include Apple Computer, Compaq, Intuit, Sybase and my company Intel. BSA websites: www.bsa.org; www.nopiracy.com.

Intel Corporation takes, as a given, that access to data communications and stored data by the intelligence and law enforcement communities is both legitimate and extremely important. But, we also recognize that there is an inevitable tide of advancing technology that renders most conventional intercept methodologies obsolete. We also believe that all American businesses need access to strong cryptography to remain competitive in an ever increasing global economy.

We believe that these varied objectives can be met if only government does not seek to force solutions on industry that are incompatible with the development of technology and market demands. It is our view that, given the breathtaking pace at which information technology (including cryptography) is developing around the globe, the only way to achieve these goals is to adopt policies that will ensure American industry leadership in the area of information technology.

This morning I would like to discuss five points that we believe should underpin U.S. encryption policy:

1. Encryption is essential to conducting all business in an Internet economy;
2. Encryption is vital to securing America's critical infrastructures;
3. The availability of encryption cannot be reasonably controlled;
4. Government promoted or required plaintext access will not work; and
5. The government needs to find technological alternatives to meet its requirements for access to information.

1. ENCRYPTION IS ESSENTIAL TO CONDUCTING ALL BUSINESS 1. IN AN INTERNET ECONOMY.

While the private sector interest in encryption export reform is generally characterized in terms of the competitiveness of American encryption products in world markets, it is, in reality, a much larger issue for American businesses. In an Internet economy, all American businesses are affected by encryption export constraints.

The future of business is fundamentally changing. The Internet presents two distinctly different business opportunities.

* *Moving existing business to the Internet.* Taking our existing paper-based commerce models and moving them to the electronic world.

* *Creating new businesses because of the Internet.* The Internet provides a ubiquity, connectivity and speed that has never existed before. There are many hereto unimagined businesses that will arise to capitalize on these capabilities.

The global economy, tied together with the Internet, is turning businesses into virtual enterprises, localized products into global products, and geographically limited networks into worldwide networks. Taking place on a massive scale, this phenomenon rests on the following business principles:

- American businesses must be able to sell and support their products worldwide.
- American businesses must be able to securely communicate and coordinate with their foreign subsidiaries and business partners worldwide.
- American businesses must be able to conduct safe electronic commerce worldwide.

I will address each of these three principles in more detail. However, it should be obvious that they all depend on secure communications and financial infrastructures. Cryptography is an essential component of the security of these critical infrastructures, regardless of the nature of the company involved.

It is easy to underestimate the magnitude of the information technology industry in the U.S. and the importance of Internet driven electronic commerce. The Department of Commerce reported that:

> *Without information technology – and the electronic commerce it fosters – overall inflation would have hit 3.1% last year, more than a full percentage point higher than the 2% it was…*[1]

By the year 2002, Internet commerce is expected to be $327 billion[2] annually. By the year 2001, the U.S. information technology industry will be directly responsible for 5% of the GNP.[3]

American businesses must be able to sell their products worldwide.

Much has been said about the need for American businesses to be able to sell their encryption products worldwide as will be discussed later in this testimony. What is not obvious is that encryption controls may make it difficult to sell non-encryption products on the world market as well. For example, a telecommunications application may need to have an integrated cryptographic component to meet an international standard.

American businesses must be able to securely communicate and coordinate with their foreign subsidiaries and business partners worldwide.

Business practices demand tight coordination with both a companies overseas subsidiaries, their suppliers and their customers. It is essential that confidentiality and access control to business information be maintained. Frequently companies are suppliers or customers on one product and competitors on another. The tightly integrated networks required for coordination could rapidly become a source of competitive intelligence if not adequately protected. Only strong cryptography can offer the level of protection required.

American businesses must be able to conduct safe electronic commerce worldwide.

In the near future, there will now longer be dedicated Internet companies – virtually every company will have to be an Internet company to survive. This requires that companies have the capability to securely sell products over the Internet to markets around the world. The ability to prevent fraud and protect intellectual property will depend heavily on the use of strong cryptography.

Importantly, corporate participation in electronic commerce includes both business-to-business and business-to-consumer transactions.

There is a need for commercial security.

There has always been some level of need for data security in commercial environments. However, the Internet has enabled the connected PC and, with it, created both new business opportunities and new security vulnerabilities.

Both the value and volume of on-line information has sharply risen. This information includes organizational information such as financial data, manufacturing information, customer information, medical and legal records, and human resources data. Additionally, there is a growing amount of data which has intrinsic value, such as monetary instruments (e.g., credit cards, coupons, etc.) and intellectual property (e.g., movies, images, etc.).

In the past, such data was protected by physical and procedural controls. The connected PC largely negates those conventional controls and requires new security mechanisms, thus creating a need for commercial security technology.

After many years of false starts, commercial data security has become a viable business. The Internet has provided the driving force for this change. Physical barriers have all but disappeared, and security perimeters have become vague.

The Internet has created needs for security that were not present in isolated security domains. This has, in turn, created opportunities for vendors of security technologies and has also created a need for standards so those technologies can interoperate.

Cryptography is the only viable solution to most commercial security requirements.

Cryptography has emerged as the only possible solution to many of the requirements of commercial security. It is the essential building block for projecting trust onto the open Internet.

The modern global commercial information infrastructure is characterized by more than 95 million Internet-connected computers,[4] most of which are in open environments with little or no physical control. They use a wide variety of hardware and software and implement no common security policy.

Only cryptographic technologies are capable of projecting security onto a completely open, arbitrary environment. Cryptography, by itself, does not guarantee any level of security. It is a necessary component but not a sufficient component.

Privacy, also known as confidentiality, is the characteristic that information is protected from being viewed in transit during communications and / or when stored in an information system. With cryptographically-provided confidentiality, encrypted information can fall into the hands of someone not authorized to view it without being compromised. It is almost entirely the confidentiality aspect of cryptography that has posed public policy dilemmas.

The commercial use of privacy (or confidentiality) encompasses not only the traditional view described above, but also the protection of intellectual property such as digital video and digital audio. The same technology used to keep communications private are required to ensure that a digital movie is not illegally copied.

ENCRYPTION IS VITAL TO SECURING AMERICA'S CRITICAL INFRASTRUCTURES.

Governments also are recognizing that without encryption, the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets remain highly vulnerable. The U.S. General Accounting Office in its report issued in May of 1996 entitled *"Information Security: Computer Attacks at Department of Defense Pose Increasing Risks"* found that computer attacks are an increasing threat, particularly through connections on the Internet, such attacks are costly and damaging, and such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

There is an awareness within the government of the vulnerability of the national information infrastructure to potential attack. The *Marsh Report*[5] highlighted the vulnerabilities very well. Much of the national economy is at risk from the decisions that are made today on the issues of infrastructure protection. Any action that degrades the security of Internet commerce or the viability of the industries involved must be viewed as a serious risk to the national security.

As the President said on January 22, 1999, before the National Academy of Sciences, "[w]e must be ready – ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services – or military assets. More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption."

The President has been so concerned that he established a Commission on Critical Infrastructure Protection to provide him with guidance and issued two Presidential Directives based on the Commission's recommendations.

In the Report of the President's Commission on Critical Infrastructure Protection entitled *Critical Foundations: Protecting America's Infrastructures* (October 1997), the Commission emphasized that "Strong encryption is an essential element for the security of the information on which critical infrastructures depend." In fact "[p]rotection of the information our critical infrastructures are increasingly dependent upon is in the national interest and essential to their evolution and full use. A secure infrastructure requires the following:

- Secure and reliable telecommunications networks.
- Effective means for protecting the information systems attached to those networks. . . .
- Effective means of protecting data against unauthorized use or disclosure.
- Well-trained users who understand how to protect their systems and data."

An earlier blue ribbon National Research Council (NRC) Committee similarly concluded in its (May 1996) CRISIS Report ("Cryptography's Role in Securing the Information Society") that encryption promotes the national security of the United States by protecting "nationally critical information systems and networks against unauthorized penetration."

Thus, the NRC Committee found that on balance the advantages of widespread encryption use outweighed the disadvantages and that the U.S. Government has "an important stake in assuring that its important and sensitive . . . information . . . is protected from foreign government or other parties whose interests are hostile to those of the United States."

In recognition of the risks and threats to information, on January 15, 1999, the National Institute of Standards and Technology (NIST) established a new draft Federal Information Processing Standard (FIPS 46-3) to require the use of stronger encryption in government systems. NIST stated that it "can no longer support the use of the DES for many applications" and that all new systems must use the significantly stronger Triple DES "to protect sensitive, unclassified data". Under the FIPS, all existing systems are now expected to develop a strategy to transition to Triple DES, with critical systems receiving a priority.

The vulnerability of national infrastructures has not been lost on other governments. Within the European Union, there is discussion on how to encourage companies to develop products to protect national infrastructures in their respective countries. Such mutual government encouragement will help to grow technical capabilities and fuel a viable world market.

Already the Swiss government is providing 128-bit encryption plug-ins for download off the Internet. The SecureNet system is required for use in accessing Telegiro, an Internet payment system. The plug-ins support SSL connections using IDEA encryption. Several Swiss banks are now using on-line banking systems compatible with the Telegiro cryptosystem.[6]

Information security is critical to the integrity, stability and health of individuals, corporations and governments. While cryptography is but one element of security, it is the keystone of secure, distributed systems. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime and sabotage through these networks. The security of any network, however, is only as good as its weakest link. America's infrastructures cannot be protected if they are networked with foreign infrastructures using weak encryption.

In the long-term, we believe it is in America's best interest to protect critical infrastructures and national security by relying on strong American encryption products. This will not happen if the U.S. Government limits the ability of U.S. companies to provide strong encryption to consumers. Indeed, the question is not whether critical infrastructures will be protected. Rather it is a question of who will protect them – U.S. or foreign companies. With individuals increasingly relying on critical infrastructures and governments increasingly desiring to safeguard these infrastructures, it is only a matter of time before strong encryption becomes a commodity feature of global networks and information systems.

*U.S. encryption export controls hurt our national security.

Our current export policy puts at risk America's global leadership in information security. U.S. export policy should, therefore, be changed so it no longer limits American participation in efforts to secure global e-commerce and related information infrastructures and no longer cedes the world market for encryption products to foreign competitors. Strong, high-quality encryption products already are widely available from foreign makers. Foreign producers of IT systems are finding that their ability to provide end-to-end systems incorporating stronger encryption than U.S. companies are permitted to export gives them a decided market advantage. We are concerned that as a result America will lose the critical encryption market to foreign companies. If that happens, it will be too late to change U.S. policy and too late to preserve U.S. leadership in this vital arena.

What will the loss of that U.S. leadership position mean? It will mean that the national security agencies will be confronting ubiquitous encryption made not by U.S. companies, but by foreign companies. Where then will the national security agencies go for technical help on encryption? It also will mean that the protection of our critical national infrastructure may depend on foreign-made systems incorporating foreign-made encryption – and that's unacceptable.

America must retain leadership in this vital technology if we are to meet our long-term national security objectives. That is why we must assess our encryption export policies from a long-term, not a short-term, perspective.

In the long run, U.S. national security objectives are best served by an IT world in which U.S. companies are market leaders in all aspects, especially encryption. U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Unfortunately, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies lose. We believe that continuing down this path will be ultimately more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

In fact, as long ago as 1996, the NRC Committee concluded that as demand for products with encryption capabilities grows worldwide, foreign competition could emerge at levels significant enough to damage the present U.S. world leadership in information technology products. The Committee felt it was important to ensure the continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including American computer, software and communications companies. Correspondingly, the Committee called for immediate and easy exportability of products meeting general commercial requirements – which is currently 128-bit level encryption!

We recognize this is a difficult balance to strike, but we strongly believe that our long term national security objectives can only be achieved if the United States realistically acknowledges the inevitability of a world of ubiquitous, strong encryption. Trying to control the proliferation of encryption is like trying to control the proliferation of mathematics. For that is what we are talking about here. Encryption algorithms are nothing but sophisticated mathematics. And while the United States may realistically hope to remain the leader in such a field, it cannot realistically expect to monopolize it.

We are joined in this view by the Center for Strategic and International Studies ("CSIS"). CSIS recently conducted a study of our nation's technical vulnerabilities; the study was chaired by William Webster, the former director of the FBI and Central Intelligence and former U.S. Circuit Judge. The subsequent report, entitled *Cybercrime… Cyberterrorism… Cyberwarfare… Averting an Electronic Waterloo*, calls for the "intelligence gathering communities – law enforcement and foreign intelligence – to examine the implications of the emerging environment and alter their traditional sources and means to address the SIW (strategic information warfare) needs of the twenty-first century. Continued reliance on limited availability of strong encryption without the development of alternative sources and means will seriously harm law enforcement and national security."

1.1 THE AVAILABILITY OF ENCRYPTION CANNOT BE REASONABLY CONTROLLED.

Cryptography is a specialized branch of mathematics. Cryptographic technology can be reduced to mathematical formulas and protocols. Information about cryptography is available from many sources and in many forms. Implementation of cryptography is no more difficult than the implementation of any complicated mathematical technology such as digital video or digital signal processing.

***Ease of implementation.**

Creation of good cryptographic algorithms that will withstand the test of time is amazingly difficult. Recent history is littered with failed attempts. Even so, many algorithms have survived and have become part of common usage. Inventing good cryptography is the mathematical equivalent of “rocket science.” Implementing those algorithms is comparably “child’s play.”

Information security is such an important part of information technology that it is rare for a graduate level computer science student to graduate without having implemented a cryptographic algorithm or protocol. Many of these students become competent systems-level programmers who could easily fashion a production-quality cryptographic application. Many of these students are non-U.S. residents.

*Open research.

Cryptography and cryptanalysis are legitimate academic research topics. There is a growing, worldwide academic community specializing in the subject. Last year alone there were over 30 international conferences focusing on cryptography or related topics and over 100 books and journals. Many of these books include detailed specifications and source code of cryptography algorithms and protocols.[7] As an example, Bruce Schneier's popular cryptography text, *Applied Cryptography,* has sold over 100,000 copies world wide.[8]

*Intangible software.

The intangible nature of cryptographic software defies any physical controls. In an instant, software, cryptographic or otherwise, can be shipped virtually anywhere in the world. As an example, within hours of the U.S. release of PGP 5.0, it was available from sites in Western Europe.[9]

Cryptography exists in many uncontrollable forms, such as general knowledge, academic research, and network deliverable software.

1.2 Availability of strong encryption products abroad.

Having export controls assumes that they are at least marginally effective. Cryptography is basically mathematics. The knowledge is inherently uncontrollable. This has led to the worldwide availability of strong encryption products and technologies.

One of the ironies of the U.S. cryptographic export regime is that it has fostered a growth in non-U.S. cryptographic technology providers who can sell strong cryptography worldwide without the constraints imposed by the U.S. government, while U.S. companies can not make the same claim.

The belief that U.S. export regulations enable foreign cryptography businesses is held by the European Commission. The EC stated at the Copenhagen Hearing:

> *The current U.S. export regulations can provide a chance for European companies to enter the market for cryptographic products. Nevertheless this would require a concentrated effort of European industry and governments to prepare the basis for this market.* .[10]

Some European companies and governments have turned this belief into practice. The following is quoted from a Siemens Nixdorf ad regarding a software product of theirs called *TrustedWeb*:

> *By simply downloading the TrustedWeb software from the Internet, you can create a highly secure Intranet infrastructure in a matter of days. The organization itself can decide on the level of security and adapt it in stages in line with needs – Ranging from simple password protection to authentication using cryptographic procedures (Public Key/Private Key) with full 128-bit key length. TrustedWeb is an independent European product and hence is not subject to the export restriction imposed by the US government in relation to encryption software.*[11]

Siemens Nixdorf runs similar ads covering their hardware products. Security products are available worldwide, in spite of, or perhaps because of, strong U.S. export controls.

1.3 Wide deployment of strong encryption is inevitable.

There are huge commercial incentives for the spread of cryptography. There is a legitimate need for the technology and a sharp increase in the amount of money being spent on security technology.[12] This has created a viable market for the technology, and there are many suppliers worldwide willing and able to meet the market demand.

The recognition of the importance of security to data communications has lead to the inclusion of security protocols within international standards. Examples of such standards include the Secure Sockets Layer (SSL) and the Internet Packet Security (IPSEC) protocols.

In most cases, the implementation of security components in international standards is optional. However, there is a strong trend to make many of these features mandatory. Thus, compliance with international communications standards will promote the diffusion of security technologies.

1. GOVERNMENT PROMOTED OR REQUIRED PLAINTEXT ACCESS
1. WILL NOT WORK.

As the spread of strong cryptography threatens traditional intelligence methods, the government has used export control relief as an incentive for companies to build plaintext access capability into every product. There have also been attempts in Congress to mandate plaintext access capability in such products. The overall approach has revolved largely, though not exclusively, around key recovery requirements. This section primarily addresses specific concerns about key recovery issues, but it is applicable to all plaintext access solutions that may be promoted or mandated by the U.S. Government (hereinafter referred to as "required plaintext access"). The basic point is that non-market driven requirements to build *any* plaintext access mechanism into products will not work.

Key recovery, as a concept, now applies not only to the initial purpose of assuring law enforcement access to encrypted materials, but also to possible end-user or organizational requirements for a mechanism to protect against lost, corrupted, or unavailable keys. It can also mean that some process, such as authority to decrypt a header containing a session key, is escrowed with a trusted party, or it can mean that a corporation or individual is ready to cooperate with law enforcement to access encrypted materials. It may also mean that some technical mechanism must be put in place to bypass the use of the key entirely (strict "plaintext access").

While required plaintext access offers, at first glance, the promises of solving the technical problems of plaintext access, it is not technically possible for it to do so in most circumstances. It is unlikely to actually meet plaintext access requirements, and its deployment as a national strategy is fraught with technical challenges and dangers.

1.1 Required plaintext access systems will not satisfy government access requirements.

Required plaintext access does not meet either law enforcement or national security requirements, but for slightly different reasons. Law enforcement can not verify compliance with key recovery requirements, and national security interests are unlikely to have access to stored keys.

*Compliance can not be verified by law enforcement.

Required plaintext access has a serious technical flaw in the area of *a priori* verification of compliance. Encryption, if applied, is likely to be applied at several different levels of the communications infrastructure. An example is having link-level encryption applied by IPSEC, having session-level encryption applied by SSL, and having application-level encryption applied by S/MIME.

Assuming one could construct a protocol to allow for the monitoring of IPSEC key recovery compliance, there is no physical way to verify that the other two levels have complied with the required plaintext access requirements unless one actually decrypts the IPSEC-data packet. If it requires probable cause to get a court order to obtain the IPSEC recovered key or mechanism, it would only be after law enforcement has probable cause of criminal activity that they would be able to verify whether or not the upper-level protocols have complied with the required plaintext access requirements.

*Required plaintext access does not address national security requirements.

While law enforcement may serve a warrant on a key recovery agent or other access mechanism provider to obtain encryption keys or the plaintext, national security interests are unlikely to have that opportunity. Required plaintext access does not provide any benefit to lawful access unless one is able to actually recover the plaintext. Targets of national security interests are unlikely to design a plaintext access infrastructure which would allow the U.S. government to have surreptitious access to stored keys or stored plaintext. This view has been born out by

National Security Agency testimony before Congress.[13]

1.2 Required plaintext access systems are of limited commercial value.

Product announcements of key recovery companies to the contrary, there is not a compelling market for commercial key recovery systems and no market for other plaintext access systems. There is no general reason to recover communications keys, and the use of key recovery for stored data ignores the fundamental properties of information.

A market for key recovery technology will emerge only when it is artificially created by government regulations. Prior to the current law enforcement push for key recovery, there were no widespread deployments of key recovery mechanisms even though the basic technology had been in existence for some time.

**Not required for data communications.*

While key recovery may, debatably, be important in certain stored data systems, in communications cryptography there is little or no user demand for this feature. In particular, there is hardly ever a reason for an encryption user to want to recover the key used to protect a communication session such as a telephone call, FAX transmission, or Internet link. If such a key is lost, corrupted, or otherwise becomes unavailable, the problem can be detected immediately and a new key negotiated.[14] There is also no reason to trust another party with such a key.

**Ignores the nature of stored data.*

Many of the proposed needs for key recovery of stored data operate under a false assumption about how data is actually stored and utilized. The frequent example is the assertion that a company will need to recover the encrypted files of an employee who has been hit by a bus.

There are three problems with this assertion. First, with the exception of personal notes, information is not solely possessed by an individual. Information is shared among a team of employees or partners in order to be of any benefit. Second, most mission-critical data is held by corporate data management systems (e.g., data bases) that have their own access control and protection mechanisms, which are administered by the corporation. Third, most personal data has a time value and rapidly becomes obsolete.

Given the observations above, we conclude that there is no business or consumer need for key recovery. Indeed, taking into account the observations and risks, Intel does not plan to implement a key recovery scheme.

1.3 Key recovery introduces additional vulnerabilities.

Centralizing all of a user's secrets or access controls in a system with increased technological and procedural operational complexities can only increase the security vulnerabilities of the operation.

Centralized attack point.

Regardless of the implementation, if key recovery systems must provide timely law enforcement access to a whole key or to plaintext, they present a new and fast path to the recovery of data that never existed before.

The key recovery access path is completely out of the control of the user. In fact, this path to lawful access is specifically designed to be concealed from the encryption user, removing one of the fundamental safeguards against the mistaken or fraudulent release of keys.

In contrast, non-recoverable systems can usually be designed securely without any alternative paths. Alternative paths to access are neither required for ordinary operation nor desirable in many applications for many users.[15]

Complexity of implementation.

Key recovery systems must be, in terms of functionally, a secure, distributed, open key management system. They have many of the properties of both large scale distributed databases and of command and control systems. Both types of systems have significant inherent complexity. As we have no practical experience, key recovery mechanisms represent a system of unknown and potentially daunting complexity.[16]

Commercial organizations would have to add the cost and risk of key recovery systems to their bottom line. Even government agencies participating in key recovery pilot programs have found the cost of centralized key recovery unacceptable.[17]

1.4 Key recovery mechanisms do not work in the horizontal information industry.

The information technology industry is characterized by an open, international, horizontal architecture. Microprocessors are sold to OEMs who build motherboards, who then contract to have BIOSs and operating systems installed. The final product is then sold to an end user who adds whatever applications they wish. New capabilities or requirements must have an active acceptance within each of the layers in order to be widely deployed. Key recovery discussion has focused only on the upper, application layer.

Low-level layers have no visibility into higher-level layers.

The nature of the information technology industry is that it is made-up of distinct horizontal architectural layers, from the microprocessor up through application programs. The components in each of these layers are supplied by different companies, having different economic models and different diffusion channels.

For valid security reasons, cryptography is migrating further “down” the layers toward the basic hardware. Key recovery, on the other hand, is a user-initiated protocol problem and can not be pushed down to the hardware. In short, cryptography implemented on hardware can not determine how it will ultimately be used.

Key recovery is under the end user's control and is performed by communications protocols or applications programs. The original microprocessor could have no knowledge of how its cryptography would be used any more than it could know how its multiplication instructions will be used.

Key recovery regulation is envisioned from the perspective of the end user. The end user "sees" a vertical single product, but the reality is that the PC is actually a collection of products from many different companies.

Horizontal interfaces are International standards.

Within the horizontal architecture of the computer industry, the interfaces between horizontal layers are defined by established international industry standards. None of these interface standards currently support key recovery of keys stored in mass market hardware. To change these standards would be a slow and difficult process.

1.5 Key recovery does not work in an international setting.

The information technology industry is based on international standards. No U.S.-only solution is commercially feasible. Most U.S. information technology companies derive a large share of their revenue from non-U.S. sources. To restrict their products to only U.S. markets would be devastating.

Not all countries will adopt key recovery.

Very few countries have embraced key recovery to the extent that the U.S. government has done. In particular, countries with strong privacy laws have generally regarded key recovery schemes as being in violation of those laws. As an example, Lotus Notes, which includes a key recovery feature, specifically lost a major sale to the Government of Sweden when the Swedish press discovered the key recovery feature.[18]

The European Commission has not endorsed key recovery as a solution to lawful access problems. It is therefore unlikely that a European-wide agreement can be reached. Indeed, the European Committee on Banking Standards (ECBS) – a powerful consortium of financial institutions – has filed a submission with the European Commission arguing against key recovery.[19]

Requires modification to existing standards.

Data communications and architectural standards are internationally-negotiated standards. None of these standards include data recovery provisions. Products must be built to conform to these standards to become mass market products. Many of these standards are not controlled by any government, rather they are controlled by commercial or user communities (such as the IETF).

Negotiating provisions for key recovery into these standards will require international agreement on the form and procedures of key recovery technology. Given the current international climate, it is unlikely that such negotiations would succeed.

Interoperability will require a non-recovery mode.

If there is even one major country which prohibits key recovery, then all developed systems will have to have a "non-key recovery" mode to facilitate interoperability. There is little that one could do to ensure that the "non-key recovery" mode was not used in normal communications.

Mutual access to keys opens U.S. companies to industrial espionage.

There is no way to guarantee that other countries will have the same level of constitutional safeguards on access to their key recovery agents as guaranteed in the U.S. U.S. corporations would be at high risk of international economic espionage if forced to deposit encryption keys with foreign key recovery agents.

According to the FBI, U.S. corporations are already targets of major industrial espionage efforts. The FBI says foreign spies have stepped up their attacks on American companies, and a new national survey estimates that intellectual property losses from foreign and domestic espionage may have exceeded $300 billion in 1997 alone.[20]

Governments of at least 23 countries, ranging from Germany to China, are targeting American companies, according to the FBI. More than 1,100 documented incidents of economic espionage and an additional 550 suspected incidents that could not be fully documented were reported last year by companies in a survey conducted by the American Society for Industrial Security.[21]

1. THE GOVERNMENT NEEDS TO FIND TECHNOLOGICAL ALTERNATIVES TO MEET ITS REQUIREMENTS FOR ACCESS TO INFORMATION.

Given the global availability of strong, non-recoverable encryption and the fast pace of technological advancement, it is clear that current US policy is not working. An alternative means to gather lawful intelligence is needed by both national security and law enforcement interests.

Clearly, Congress should adequately fund the technical efforts of our law enforcement and national security agencies so they can meet these challenges. And industry would support additional funding.

For example, ACP, for example, has advocated that the U.S. Government should work cooperatively with our nation's hardware and software manufacturers to develop the technical tools and know-how to achieve a policy that effectively responds to society's needs for law enforcement, national security, critical infrastructure protection, privacy preservation, and economic well-being.

1.1 NET center proposal.

Last year, ACP proposed the creation of a National Center for Secure Network Communications ("NET Center"). The NET Center (now called "Tech Center") concept is aimed at helping law enforcement officials to understand how to deal with encryption and other technical advances when encountered in a criminal setting.

The Tech Center should be a public-private entity operating within a national laboratory for information technology to perform research and act as a forum for further discussions on technology trends and vulnerabilities. Clearly a Tech Center must operate within a legal framework that provides reasonable safeguards.

Attorney General Janet Reno announced plans for the Federal Bureau of Investigation to set up a new $64 million center to protect the nation's critical infrastructures, particularly computer networks, from both physical and cyber attack.

1.2 Industry cooperation.

The national security is best secured by the American companies actively competing for and supplying the fundamental technologies of the national infrastructure. Only those companies directly involved in the research and development of information technology components can assess the security and vulnerabilities of the infrastructures created from those components. Technical innovation is predominantly centered in the private sector. Only a government/industry cooperation can effectively address the challenge of continued technological change.

1. CONCLUSION: THE PROTECT ACT SHOULD BE PASSED
1. WITH FURTHER IMPROVEMENTS

The mass market model.

Mass-market hardware manufacturers and software publishers sell products through multiple distribution channels such as OEMs (*i.e.*, hardware manufacturers that pre-load software onto computers), value-added resellers, retail stores and the emerging channel of on-line distribution. Thus, mass market products are available to the general public from a variety of sources.

The mass-market distribution model presupposes that hardware manufacturers and software publishers will take full advantage of these multiple channels to ship identical or substantially similar products worldwide (allowing only for differences resulting from localization) irrespective of specific customer location or characteristics. As mass market products are uncontrollable, Intel believes U.S. companies should be able to export the current market standard of 128-bit encryption. Unfortunately, the Administration only permits easy exports of 56-bit encryption even if foreign products exist in the marketplace. And the Administration continues to impose onerous controls on 56-bit toolkits and hardware encryption components, notably semiconductors.

The PROTECT Act grants export control relief to products at all horizontal levels.

Intel believes that all distinct horizontal architectural layers, from the microprocessor up through application programs should be treated identically under any encryption export policy. However, contrary to the Administration's original announcement regarding export relief which included export relief for hardware, the new regulations still do not permit 56-bit encryption chips, integrated circuits, toolkits and executable or linkable modules to be easily exported except to subsidiaries of U.S. companies or otherwise relax export controls on stronger mass market hardware. We are pleased that the PROTECT Act remedies this problem and treats mass market hardware in the same manner as mass market software.

The PROTECT Act eliminates reporting requirements for mass market products.

We are encouraged that the PROTECT Act recognizes the difficulties in complying with reporting requirements for mass market encryption products and eliminates such reporting requirements. It is virtually impossible for mass-market exporters to report the name and address of each end-user. Millions of these products are sold through multi-level distribution channels (*e.g.*, VAR's and chain stores). Moreover, as registration of mass market products is customarily voluntary. This is a vast improvement over the Administration's proposed regulations which effectively require companies to develop a system to obtain the names and addresses for each health and medical end-user of stronger encryption products and all foreign online merchants.

The PROTECT Act's export relief for mass market products and for products which face competition from comparable foreign products is too complicated and creates an unwieldy bureaucracy.

We are pleased that the PROTECT Act does recognize that mass market and publicly available encryption products, and encryption products for which comparable foreign products are available, should be treated differently under the U.S. export regime. The bill acknowledges the futility of trying to control a product that can be bought off of the Internet or easily purchased from commercial vendors such as CompUSA or from Circuit City by any individual in America regardless of nationality, or a comparable product can be easily purchased from similar stores in a foreign country. "Bad guys" certainly will have no problems obtaining the encryption products, and no concerns about "exporting" the products via telephone lines or the Internet or smuggled out on personally pressed CDs. The only impact of the export controls will be to stop American companies from selling American products to legitimate users.

Unfortunately, the PROTECT Act establishes a complicated private/public board structure for deciding after-the-fact whether or not a product is a mass market product or whether comparable foreign products are available. The Secretary of Commerce has thirty days to approve or disapprove the Board determination, subject to judicial review, and the President may override any determination. There is no guarantee of any consistency in the Board's decisions. Thus, while the Board procedure is an improvement, and the opportunity for judicial review provides a mechanism to ensure that exports are not denied in an arbitrary and capricious manner, it is not a predictable, clear process giving American companies certainty as to whether they can export their products. Such predictability is necessary so that American companies can have confidence designing and building security features into their products.

The PROTECT Act should, but does not, afford complete and immediate export relief for mass market encryption without any complicated oversight. The Act also does not recognize that if a comparable foreign product is available, *any* delay in exports provides a significant advantage to the foreign product.

The PROTECT Act supports development of AES, but delays full export control relief until 2002.

The PROTECT Act also provides Congressional support for, and sets a 5-year limit on the selection of, the 128-bit Advanced Encryption Standard which is being developed under the auspices of the National Institute of Standards and Technology. The 2002 deadline will provide impetus for NIST to finish developing the standard in a timely manner while providing NIST with sufficient time to study the final standard's security features. This is an important process that will result in a new standard for government's sensitive, but unclassified, information and most likely will serve as the new worldwide standard for strong encryption similar to the Data Encryption Standard when it was introduced in the 1970's. Once the algorithm is selected, the PROTECT Act removes all export controls on encryption products using the 128-bit standard or its equivalent strength.

Unfortunately, because the PROTECT Act limits easy exportability of mass market products until the AES is adopted, general distribution of these products will have to wait almost three years. Considering the current speed of technological change, where Internet products are now on three-month product cycle times, and the fact that 128-bit comparable foreign encryption is currently available, this is an eternity in Internet time. Law enforcement and national security interests have known for a long time that ubiquitous use of strong encryption by consumers worldwide is just around the corner. They cannot hope to continue to delay the world from using strong encryption according to their timeframe.

1. A new approach.

The preceding has made the argument that:

- Encryption is essential to conducting all business in an Internet economy;
- Encryption is vital to securing America's critical infrastructures;
- The availability of encryption cannot be reasonably controlled;
- Government promoted or required plaintext access will not work; and
- The government needs to find technological alternatives to meet its requirements for access to information.

If accepted, these arguments force one to the conclusion that a new approach to encryption policy is required.

[1] Wall Street Journal, *Department of Commerce talks about Inflation*, 16 April 1998.
[2] Forrester Research
[3] Dataquest
[4] Ibid., p. 8.
[5] Marsh, R., Chairman, *Critical Foundations: Protecting America's Infrastructure*, The President's Commission on Critical Infrastructure Protection, October 1997.
[6] See http://www.swisspost.ch/E/21.html
[7] Schneier, B., *Applied Cryptography*, John Wiley & Sons, Inc., New York, NY, 1996.
[8] Schneier, B., Private correspondence, June 1998.
[9] Hayward, D., *Europeans Break Encryption Barriers, TechWire*, 17 June 1997.
[10] Ministry of Research and Information Technology Denmark for the European Commission Directorate-General XIII Telecommunications, Information Market and Exploitation of Research, *Report of Day 1 of the European Expert Hearing on Digital Signatures and Encryption (Copenhagen, April 23, 1998)*, Copenhagen, Denmark, 23-24 April 1998
[11] Siemens Nixdorf, Press Release, http://www.trustedweb.com/whats_new/pressrelease.html, Hanover, Germany.
[12] Burnahm, B., *The Electronic Commerce Report*, Piper Jaffray Research, p. 75, August 1997.
[13] Crowell, W., Deputy Director National Security Agency, Testimony before Senate Commerce Committee, 1997.
[14] Neumann, P., et.al., *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption*, Final Report of The Cryptographers' Working Group, 27 May 1997.
[15] Ibid.
[16] Ibid.
[17] Wayner, P., *Administration Gets Sour Taste From Own Encryption Medicine*, New York Times, 1 July 1997.
[18] Laurin, F., and Froste, C., *Secret Swedish E-Mail Can Be Read by the U.S.A.*, Svenska Dagbladet, 18 Nov 1997.
[19] Computing, *Banks Slam Snoops*, 26 March 1998.
[20] Nelson, J., *FBI: Commercial Spying Rises*, Los Angeles Times, 12 January 1998.
[21] Ibid.